Federal Defenders
OF NEW YORK, INC.

Southern District
52 Duane Street-10th Floor, New York, NY 10007
Tel: (212) 417-8700 Fax: (212) 571-0392

David E. Patton
Executive Director

Southern District of New York
Jennifer L. Brown
Attorney-in-Charge

February 22, 2020

BY ECF

Hon. Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: *United States v. Schulte*,
S2 17 Cr. 548 (PAC)

Dear Judge Crotty:

Defendant Joshua Adam Schulte submits this reply in further support of his motion for a mistrial.

1. The government's *Brady* violations require a mistrial.

The government improperly suppressed *Brady/Giglio* material related to a CIA employee and government witness known to the jury as "Michael." For the reasons explained in the defense's initial motion, the Court should order a mistrial.

The government's February 19, 2020 opposition ("Gov't Opp.") rests on a fundamental misapprehension. According to the government, "[n]either the Government nor the CIA believes anyone" other than Mr. Schulte was involved in the charged disclosures, *see* Gov't Opp. at 1, and therefore, there is no *Brady* violation. Regardless of the government's belief about who committed a charged crime, a defendant is constitutionally entitled to present evidence of alternative suspects, and the government is legally obligated to disclose materials in its possession suggesting that someone else may have committed the crime.

The defense must receive this information from the government in time for its effective use at trial. *See, e.g.*, *Leka v. Portuondo*, 257 F.3d 89, 103 (2d Cir. 2001) ("The opportunity for use under *Brady* is the opportunity for a responsible lawyer to use the information with some degree of calculation and forethought."). *See also United States v. Djibo*, 730 F. App'x 52, 56 (2d Cir. 2018) (summary order) (finding

court abused its discretion in denying new trial where it did not give defendant sufficient time to review late government disclosure that possibly contained exculpatory evidence); *United States v. Robert Pizarro*, No. 17 Cr. 151 (AJN), ECF Docket No. 135 (S.D.N.Y. May 17, 2018) (postponing trial, over government objection, and criticizing SDNY prosecutors for delaying production of evidence of a possible alternative perpetrator of the crime until the Friday before the start of trial; noting irrelevance of fact that government believed defendant, and not this possible alternative perpetrator, committed the crime); *United States v. Reichberg*, No. 16 Cr. 468 (GHW), 2018 WL 6599465, at *3-4 (S.D.N.Y. Dec. 14, 2018) (describing earlier trial postponement that was necessary because SDNY prosecutors delayed producing *Brady* material until five days before the start of trial); *United States v. Russell*, No. 16 Cr. 396 (GHW), 2018 WL 2088282, at *1-2 (S.D.N.Y. May 4, 2018) (granting new trial based on SDNY prosecutors' "inadvertent" failure to disclose proffer notes, which would have "provided substantial grist for cross-examination" of witness and impeachment).

Yet in this case, the government withheld material information from the defense until after the trial had already started, waiting until the literal eve of Michael's testimony. Even then, the government did not make a full disclosure of all of the relevant information in its possession: a more complete disclosure came only after the Court undertook an *in camera* review of the CIA Memorandum and, later, Michael's investigative file. And the investigative file reveals even more *Brady/Giglio* material that the government had not produced. If the government withheld all of this crucial material about Michael's potential culpability and dishonesty until the Court took action, what else is it hiding?

The government seeks to excuse its misconduct because the CIA Memorandum supposedly merely "questioned Michael's credibility," and because "that type of opinion evidence is inadmissible as a matter of law." Gov't Opp. at 14. The government is wrong on both counts. First, the CIA did not simply "question" Michael's veracity: it determined, *inter alia*, that he is an immediate security risk. In any event, the government's obligations under *Brady* and *Giglio* required disclosure *whether or not* the government believed the CIA Memorandum was admissible. *See United States v. Rodriguez*, 496 F.3d 221, 226 & n.4 (2d Cir. 2007) ("The obligation to disclose information covered by the *Brady* and *Giglio* rules exists without regard to whether that information has been recorded in tangible form." Further, it "*does not depend on whether the information to be disclosed is admissible as evidence in its present form*.The objectives of fairness to the defendant, as well as the legal system's objective of convicting the guilty rather than the innocent, require that the prosecution make the defense aware of material information potentially leading to admissible evidence favorable to the defense.") (emphasis added).

The government also claims that its misconduct is of no consequence because Michael did not have the ability to access the "Altabackups" from which the Vault 7 material was allegedly copied. As Dr. Bellovin's annexed declaration demonstrates, Michael did indeed have the ability to access those files—thereby underscoring his potential culpability and the significance of the government's *Brady* violations.

Nor is the government correct that its mid-trial disclosures contained no new information. It was only mid-trial that the defense learned that Michael was on administrative leave because of his suspicious conduct during this investigation (a fact that may be relevant to both his possible involvement in the charged crime and impeachment) and that he had failed two polygraph tests in connection with this case. *See United States v. Banks*, 546 F.3d 507 (7th Cir. 2008) (information that DEA chemist was being investigated for misuse of government credit card, which could have been used to impeach her, was material, and the defendant was prejudiced by the government's nondisclosure). In addition, the government's mid-trial disclosures have revealed more about the suspicious screenshot that Michael took, and provided evidence of a possible connection between Michael and a specific named individual at [redacted]

All of this information should have been disclosed to the defense well in advance of trial. Defense counsel cannot suddenly accuse a third person—Michael—of being the real perpetrator of the crimes in the fourth week of trial. To be effective, such a serious accusation should have been presented to the jury at the outset—in the defense's opening statement—and reiterated through the questioning of every witness with potential knowledge of Michael's activity. For the reasons described in the defense's initial motion, the government's delayed disclosures have prevented the defense from effectively using the newly revealed material at trial, and the only effective remedy at this point is for the Court to declare a mistrial.

2. The government should have produced the mirror images requested by the defense and its failure to do so requires a mistrial.

The government spills much ink trying to justify its failure to produce full forensic "mirror" images of the ESXi Server and FS01 Server to the defense. But the bottom line is this: the government produced these mirror images to its own outside forensic expert, Patrick Leedom, and that expert relied upon those mirror images in conducting his forensic analysis, forming his expert opinions, and giving his testimony at trial. *See* Tr. 1159-60, 1186-87. In light of these clear, undisputed facts, due process, the Sixth Amendment, and Rule 16 required the government to provide those mirror images to the defense. Its failure to do so warrants a mistrial.

The government seeks to obfuscate these simple facts by listing other disclosures it made to the defense. In its prior submission, the defense thoroughly explained why these more limited disclosures were not sufficient. In the annexed declaration, Dr. Bellovin further explains why these disclosures were deficient. And, again, the simple fact is that the government itself conceded the materiality and importance of the actual mirror images when it provided them to its own outside expert. In a criminal case, a defense expert is entitled to the same access to available evidence as a government expert. "Access provided to private experts retained by the prosecution must be provided to private experts retained by the defense." *United States v. Shrake,* 515 F.3d 743, 747 (7th Cir. 2008) (citing *Wardius v. Oregon,* 412 U.S. 470 (1973)). This principle is not new: in drug cases, the defense is permitted to conduct its own independent testing to verify that something is a controlled substance. *See, e.g.*, *United States v. Butler*, 988 F.2d 537, 543–44 (5th Cir. 1993) (finding error and vacating conviction where district court refused to let defendant test controlled substance, noting that a "concomitant part" of the defense's right to examine the government's evidence "is the right of the accused to have an independent chemical analysis performed on the seized substance"). Similarly, when the government seeks to rely on DNA evidence, the defense can hire an expert to conduct her own independent testing of that evidence. The Court would not permit the government to deny the defense expert access to available drug or DNA evidence that the government's expert had examined; nor would the Court insist that the defense rely upon the government expert's analysis. Yet that is what the government is asking here.

This is not a situation where the defense seeks some sort of unfettered access to the government's investigative files. The defense is only seeking the same access to underlying evidence as the government's own outside expert.

In addition, when evidence in a criminal case involves electronic media, the Second Circuit has explicitly recognized the importance of the defense having access to a full mirror image or complete forensic copy of the media—not just certain files chosen by the government. In *United States v. Ganias*, in explaining why the government needed to retain original copies or full mirror images of electronic media, the Circuit noted:

> Retention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved. … Defendants may also require access to a forensic copy to conduct an independent analysis of precisely what the government's forensic expert did—potentially altering evidence in a manner material to the case—or to locate exculpatory evidence that the government missed.

824 F.3d 199, 215 (2d Cir. 2016) (en banc). *Ganias* explains why full mirror images of electronic media should be retained by the government—and why they should be provided to the defense. In the words of the Second Circuit, the defense must be able to conduct its own "independent analysis of precisely what the government's forensic expert did" for various reasons, including that the government's expert may have "alter[ed] evidence in a manner material to the case" or may have missed "exculpatory evidence." *Id.*; *see also id.* at 215 n.35 (collecting authorities emphasizing defense need to conduct its own independent analysis of full forensic record). Because the defense was denied access to the same mirror images reviewed by the government's expert, it was unable to perform the sort of complete analysis contemplated by the Second Circuit. *Cf. United States v. Aleynikov*, 785 F. Supp. 2d 46, 77 (S.D.N.Y. 2011) (denying motion for new trial because "[b]oth experts were given only the source code stolen by Aleynikov and thus were *operating on a level playing field*") (emphasis added), *rev'd on other grounds*, 676 F.3d 71 (2d Cir. 2012).

Ganias also explains why the process that the government followed here is inadequate: "extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium. Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence …." 824 F.3d at 215.

Nor can the government evade its disclosure obligations by resorting to claims of national security concerns. Presumably, when the government was litigating this issue pretrial in its *ex parte* submissions, it did not disclose to this Court that it had provided its own outside expert with the mirror images sought by the defense. The government's expert, Mr. Leedom, is not a member of the CIA or a government employee. From a security perspective, he is on equal footing with the defense's independent expert. If national security allows for providing these images to Mr. Leedom, there can be no national security basis to withhold them from the defense.

In sum, the *Brady* violations and the ongoing failure to provide the mirror images to the defense, whether viewed singly or, especially, in combination, have rendered this trial fundamentally unfair. A mistrial is necessary.

Respectfully submitted,

___/s/_____
Sabrina Shroff
Edward Zas
Attorneys for Joshua Schulte

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA :

S2 17 Cr. 548 (PAC)

-v- :

JOSHUA ADAM SCHULTE,

Defendant. :

----------X

DECLARATION OF STEVEN M. BELLOVIN, Ph.D.

STEVEN M. BELLOVIN, Ph.D., declares under penalty of perjury:

1. I am the Percy K. and Vida L.W. Hudson Professor of Computer Science and affiliate law faculty at Columbia University. I was retained by defense counsel in this case to assist as an expert in computer systems and computer security. I make this declaration in support of Mr. Schulte's motion for a mistrial and, more specifically, to reply to some of the points made by the government in opposition to that motion. This declaration is based on my personal knowledge and more than 50 years of experience as a computer expert.

2. I have reviewed the government's letter to the Court, dated February 19, 2020, opposing Mr. Schulte's motion for a mistrial ("Gov't Opp."). The government claims, in summary, that the defense has not been prejudiced by the government's decision to grant its forensic expert Patrick Leedom—but

not me or defense counsel—access to the "mirror images" of the CIA's ESXi Server and NetApp Server (also known as the FSO1 Server). The government asserts that "the defense has had all of the information upon which Mr. Leedom relied to arrive at his opinions well before trial, and thus a reasonable opportunity to test and scrutinize those opinions." Gov't Opp. at 14.

3. The government's assertions are not accurate. As discussed below, because I was never granted access to the mirror images, I have been unable to reproduce (and thereby confirm or refute) all the analyses and tests that Mr. Leedom was able to perform. While the government notes that it has made a substantial amount of forensic material available to the defense, this material is far from complete, and is not usable to conduct certain analyses that the government's expert was able to conduct. Those analyses require examination of the mirror images.

4. The government makes a number of specific assertions that are misleading or simply false. For example, the government states that certain FBI reports "make clear that Michael never had Atlassian administrator privileges and thus did not have the ability to access or copy the Altabackups (from which the Vault 7 information was stolen)." Gov't Opp. at 8. As a simple factual matter, this statement is untrue. The possession of "Atlassian administrator privileges" had nothing to do with the ability to access or copy the Altabackup files. Rather, what was needed was *log-in access*, i.e., a working user name

and password, to the Confluence Virtual Machine (or "VM"). Michael certainly had such log-in access. As shown in Leedom Slide 60 (GX 1207-10 and GX 1207-11), which is described as "April 16, 2016 Confluence Backup—password and shadow files," a user name called "confluence" is listed (Slide 60, GX 1207-11, third line from the bottom). The password for this user name was listed on a web page that was accessible to all OSB members, including Michael, and was used for many other log-ins throughout the organization. *See* GX 1202-5 (listing one commonly used password as "123ABCdef."). This password was valid both before and after April 16, 2016. So if Michael had simply typed that password into the Confluence VM on April 20, 2016, along with the user name "confluence," he would have had access to the Altabackup files from which the Vault 7 information was allegedly taken.

5. Any experienced computer programmer would have known that there was very likely to be a user name "confluence" on the Confluence VM. On Linux systems, it is normal to have a separate user name for any software packages that manage their own data; this includes Confluence and all other elements of the Atlassian software suite. There are several other examples of this in just the Confluence password and shadow files. It is customary to use the name of the software package, e.g., "confluence" as the user name. Again, this is evident on the Confluence VM itself.

6. The above point demonstrates, contrary to the government's assertions, that Michael had the ability to access and copy the March 3, 2016 Confluence and

Stash backup files that the government claims were eventually sent to WikiLeaks.

7. The government also asserts that it has provided large amounts of information to the defense, including log files, but this data is in no way equivalent to the information to which Mr. Leedom has had access.

8. The government claims that it gave the defense log files from the ESXi server. In fact—per the defense *ex parte* letter to the Court of February 12, 2019—some of those files were demonstrably damaged. Such damage was likely the result of prior forensic examination, which the government was able to perform on the original image of the server. Had the defense been provided with a full mirror image of the ESXi server, the defense would have been able to conduct its own examination of the files in their original state.

9. The government claims that it provided the Confluence databases to the defense. But those databases appear to have been heavily redacted, with all content files either missing or deleted, including those allegedly released by WikiLeaks. Furthermore, they did not include the apparently damaged "SQL" file that Mr. Berger evidently used in his analyses. GX 1704, Slide 3 (GX 1207-97). If the defense had a full copy of the SQL file—not simply a file embedded as part of a forensic case—the defense could have done other SQL queries to establish whether the data could have been taken from a later backup file.

10. The government claims that defense had the "backup script" in sufficient time to determine whether Mr. Leedom's claims about the damage to the SQL file are accurate. In fact, without access the mirror images, and for reasons too complex and technical to explain here, the backup script alone does not permit the defense to assess the validity of all of Mr. Leedom's assertions.

11. The government claims that it has produced to the defense all of the unallocated space from the ESXi server "about which Mr. Leedom testified." Gov't Opp. at 19 ¶ 6. But "the unallocated space …about which Mr. Leedom *testified*" (emphasis added) is not the same as all the unallocated space he *examined*. If I had been granted access to the examined space, there is a reasonable probability I would have discovered evidence, including potentially exculpatory evidence, that Mr. Leedom either missed or ignored.

I declare under penalty of perjury that the foregoing is true and correct.

/s/

Steven M. Bellovin, Ph.D.

February 22, 2020